SANOVIS CONSULTING WITH CARE.

CURACON SICHERHEIT GEBEN. LÖSUNGEN BIETEN.

NEWSLETTER DATENSCHUTZ

Liebe Leserin, lieber Leser,

nicht nur durch die Corona-Pandemie erlebt die IT und damit auch der Datenschutz viele Veränderungen. Im rechtlichen Bereich gibt es ebenfalls Entwicklungen, die den Schutz personenbezogener Daten betreffen. Ihr Datenschutz-Newsletter bringt Sie auf den aktuellen Stand.

So wandelt sich die Arbeitswelt erneut, Beschäftigte kehren teilweise aus dem Homeoffice in ihr Büro zurück oder pendeln zwischen den Arbeitsorten. Für den Datenschutz bedeutet dies, dass sowohl die Maßnahmen für sichere Datenzugriffe als auch der Schutz vertraulicher Papierdokumente angepasst werden müssen.

Zudem gibt es eine neue Rechtsprechung zum Auskunftsrecht nach der Datenschutz-Grundverordnung und eine neue Rechtsgrundlage für Daten-übermittlungen in Staaten außerhalb der EU. Erfahren Sie, was das für Ihre tägliche Arbeit bedeuten kann.

Wir wünschen Ihnen interessante Erkenntnisse beim Lesen!

Dr. Uwe Günther
Beratungsfeldleiter Datenschutz, Curacon GmbH
Geschäftsführer, Sanovis GmbH

Stefan Strüwe
Beratungsfeldleiter Datenschutz, Curacon GmbH

August_2021

1 WIE SIE EIN VPN EINRICHTEN UND NUTZEN

Ob im Homeoffice oder unterwegs: Für den Zugriff auf das Unternehmensnetzwerk soll nicht das offene Internet, sondern ein Virtual Private Network (VPN) genutzt werden. Doch wie funktioniert das in der Praxis? Lesen Sie wichtige Hinweise zur Einrichtung und Nutzung.

Flexible Arbeit hat Folgen für den Datenschutz

Nach dem Ende der Homeoffice-Pflicht sind bereits viele Beschäftigte in ihr bisheriges Büro zurückgekehrt. In vielen Fällen besteht aber weiterhin die Möglichkeit, zeitweise im Homeoffice zu arbeiten. Gleichzeitig finden wieder mehr Vor-Ort-Termine statt. Dadurch nimmt die mobile Arbeit wieder zu.

Die flexible Arbeitsumgebung hat aber Konsequenzen für den Schutz personenbezogener Daten. Die Datenrisiken im Büro, im Homeoffice und unterwegs können sehr verschieden sein. Die Maßnahmen für den Datenschutz sollten den jeweiligen Schutzbedarf berücksichtigen und damit auch den Arbeitsort.

Eines aber haben die Arbeitsorte außerhalb des Büros gemeinsam: Ist ein Zugriff auf das Unternehmens-netzwerk, auf betriebliche Applikationen oder auf Daten in der Unternehmens-Cloud nötig, kommt ein Dienst zum Aufbau eines VPN (Virtual Private Network) ins Spiel.

Sicherer Netzwerkzugang mit Virtual Private Networks

Nutzen Sie im Homeoffice oder bei der mobilen Arbeit VPN, kommt es zuerst einmal darauf an, den richtigen, vom Unternehmen freigegebenen VPN-Dienst zu verwenden. Im Internet kursieren viele Angebote für kostenlose VPN-Dienste. Doch VPN kann gegen Lauschangriffe durch Dritte auf die Verbindung zum Unternehmen schützen, nicht aber gegen denkbare Zugriffe durch den VPN-Anbieter selbst.

Es ist deshalb entscheidend, einen vertrauenswürdigen, sicheren VPN-Dienst einzusetzen. Die Auswahl trifft Ihr Arbeitgeber, nachdem er den VPN-Service geprüft hat. Sie selbst als Nutzer sollten deshalb keinen anderen VPN-Dienst als den jeweils freigegebenen verwenden. Wissen Sie nicht, welcher das ist, fragen Sie danach bei der im Unternehmen zuständigen Stelle.

VPN im Homeoffice

Sind Sie im Homeoffice tätig und wollen auf das Unternehmensnetzwerk zugreifen, verwenden Sie den VPN-Dienst in aller Regel über Ihren Desktop-PC oder Ihr Notebook. Je nach VPN-Service wird dazu einmalig ein VPN-Client auf dem Endgerät eingerichtet, der VPN-Dienst im Browser oder im Internet-Router konfiguriert oder in den Betriebssystemeinstellungen. Fragen Sie Ihre IT-Administration nach der entsprechenden Anleitung.

Wichtig ist, dass Sie das eingerichtete VPN auch nutzen. Dazu müssen Sie die VPN-Verbindung entsprechend aktivieren. Andernfalls haben Sie zwar die Voraussetzungen für VPN, nutzen aber trotzdem das offene Internet.

VPN unterwegs

Auch außerhalb des Homeoffice, zum Beispiel auf dem Weg vom Homeoffice in Ihr Büro im Unternehmen, kann es notwendig sein, mit Ihrem mobilen Endgerät auf das Firmennetzwerk oder auf betriebliche Cloud-Dienste zuzugreifen. Dazu sollte Ihr Smartphone oder Tablet entsprechend eingerichtet sein. Je nach VPN-Dienst gibt es dazu eine spezielle VPN-App, die Sie dann jeweils zuerst starten müssen, wenn Sie sich bei Firmensystemen anmelden wollen.

2 KOSTENLOSE MUSTER DER EU FÜR DATENSCHUTZVERTRÄGE

Kostenlose Vertragsmuster, frei verwendbar – das bietet die EU für die Auftragsverarbeitung und für die Datenübermittlung in „Drittstaaten“ wie die USA. Diese nützlichen Arbeitsinstrumente sollte man kennen.

Dokumentation ist alles

Verträge über die Verarbeitung von personenbezogenen Daten müssen dokumentiert sein. Mündliche Verträge reichen nicht. Das ist allgemein bekannt. Denn sonst lässt sich nicht nachweisen, dass der Datenschutz eingehalten ist. Aber wo findet man rechtssichere Muster? Für zwei wichtige Konstellationen fällt die Antwort inzwischen leicht: Im Juni 2021 hat die Europäische Kommission offizielle Vertragsmus-ter veröffentlicht, die sich mit den beiden Themen „Datenübermittlung in Drittstaaten“ und „Auftragsverar-beitung“ befassen.

Die Vertragsmuster sind frei verfügbar

Diese Muster darf jeder frei verwenden. Das verletzt in keiner Weise irgendein Urheberrecht. Die Muster stehen kostenlos zur Verfügung. Und zwar in allen 24 Amtssprachen der EU. Alles in offizieller Überset-zung, angefertigt von den Profis des EU-Übersetzungsdienstes. Vorlagen dieser Qualität könnten selbst große Unternehmen nur mit enormem Aufwand erstellen. Es handelt sich also um einen erheblichen Service der EU-Kommission.

Es gibt „sichere“ und „unsichere“ Drittstaaten

Ein Set von Musterverträgen befasst sich mit der Datenübermittlung in Drittstaaten. Drittstaaten sind alle Staaten, die kein Mitglied der EU sind. Für manche dieser Drittstaaten hat die Europäische Kommission offiziell festgestellt, dass sie gewissermaßen als „datenschutzrechtlich sicher“ gelten. Das ist etwa bei der Schweiz oder auch bei Japan der Fall. Für die meisten Drittstaaten gibt es eine solche Feststellung aber nicht. Wichtigstes Beispiel hierfür sind die USA.

Die Muster sorgen für Rechtssicherheit

Bei diesen „unsicheren“ Drittstaaten braucht man besondere Rechtsgrundlagen, um personenbezogene Daten an Unternehmen in diesen Staaten übermitteln zu dürfen. Ein wichtiges Rechtsinstrument hierfür sind die „EU-Standardvertragsklauseln“. Sie können verwendet werden, wenn ein Unternehmen in der EU personenbezogene Daten an Unternehmen in einen „unsicheren“ Drittstaat übermittelt.

Stichtag für die neuen Muster war der 27.6.2021

Die bisherigen Musterverträge der EU für die Übermittlung in Drittstaaten waren schon über zehn Jahre alt. In dieser Zeit gab es viele neue technische, aber auch rechtliche Entwicklungen. Schon deshalb war es notwendig, die Musterverträge anzupassen. Das ist jetzt geschehen. Seit dem 27.6.2021 sind die neuen Vorlagen maßgeblich. Verträge auf der Basis der alten Vertragsmuster müssen bis zum 27. Dezember 2022 angepasst werden.

Völlig neu: Vertragsmuster für die Auftragsverarbeitung

Völlig neu ist das Set von Musterverträgen für die Auftragsverarbeitung. Die Auftragsverarbeitung kommt vor allem ins Spiel, wenn ein Unternehmen externe Dienstleister einschaltet. Sie brauchen oft personenbezogene Daten von Kunden oder auch Mitarbeitern. Das sind typische Anwendungsfälle der Auftragsverarbeitung.

Sie passen auch innerhalb Deutschlands

Für die neuen „Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern“ ist es gleichgültig, ob der Dienstleister in Deutschland ansässig ist oder sonst wo in der EU. Sie sind gerade für den Fall gedacht, dass zwei Unternehmen innerhalb der EU eine Auftragsverarbeitung vereinbaren. Aber auch wenn die beteiligten Unternehmen in Deutschland ansässig sind, können sie die Klauseln verwenden.

Sollte der Auftragsverarbeiter dagegen in einem Drittstaat ansässig sein, kommen die Standardvertragsklauseln für die Datenübermittlung in Drittstaaten zur Anwendung. Sie decken den besonderen Fall der Auftragsverarbeitung gewissermaßen mit ab.

Der „modulare Aufbau“ macht vieles leichter

Eine wichtige Neuerung bei allen Vertragsmustern ist der „modulare Aufbau“. Er soll ihre Anwendung so einfach wie möglich machen. Er prägt besonders die Vertragsmuster für die Übermittlung in Drittländer. Dort sind vier Module vorgesehen. Sie gehen auf die jeweilige Situation der beteiligten Unternehmen ein.

So erfasst Modul 1 die Situation, dass die beteiligten Unternehmen sich sozusagen auf Augenhöhe gegenüberstehen. Dies ist dann der Fall, wenn die Datenübermittlung zwischen zwei gleichberechtigten Verantwortlichen stattfindet. Modul 2 passt dagegen für die Situation, dass ein Unternehmen in der EU Daten an einen Auftragsverarbeiter in einem Drittstaat übermittelt. Die Wahl des richtigen Moduls ist viel einfacher, als es zunächst wirkt. Und dann kann man gleich anfangen, das Vertragsmuster auszufüllen.

3 DIE ZWEI SEITEN DES AUSKUNFTSANSPRUCHS

Alle haben Anspruch auf Auskunft über ihre personenbezogenen Daten. Das sieht die DSGVO so vor. Der Bundesgerichtshof legt den Anspruch sehr weit aus. Das ist schön, wenn man selbst Auskunft haben möchte. Es kann aber viel Arbeit machen, wenn man im Unternehmen eine Auskunft vorbereiten muss.

Der Auskunftsanspruch hat zwei Stufen

Der Auskunftsanspruch ist ein zentrales Element des Datenschutzes. Jeder soll erfahren können, was beispielsweise ein Unternehmen über ihn weiß. Der Anspruch besteht aus zwei Stufen. In Stufe 1 kann die betroffene Person Auskunft darüber verlangen, ob überhaupt Daten verarbeitet werden, die sie betreffen. Ist das nicht der Fall, lautet die Antwort nein. Ist es der Fall, lautet die Antwort dagegen ja.

Der Personenbezug von Daten reicht weit

Beim „Ja-Fall“ schließt sich Stufe 2 des Anspruchs an. Dann kann die betroffene Person Auskunft über alle Daten verlangen, die sie betreffen. Das geht sehr weit. Erfasst ist wirklich alles, was über eine Person vorliegt. Der Bundesgerichtshof hat dies am Beispiel einer Lebensversicherung deutlich gemacht. Demnach umfasst der Anspruch beispielsweise:

- den gesamten Schriftwechsel zwischen der Versicherung und dem Versicherten
- alle Daten des Versicherungskontos
- alle Telefonnotizen und Gesprächsvermerke, die Fakten über die versicherte Person enthalten

Auf Papier oder elektronisch macht keinen Unterschied

Der Anspruch umfasst also weit mehr als das, was die „Versicherungsakte“ enthält, die unter dem Namen des Versicherten geführt wird. Es spielt auch keine Rolle, ob etwa eine Telefonnotiz elektronisch festgehalten ist oder auf Papier. Auch wenn sie als Zettel im Schreibtisch des Sachbearbeiters liegt, gehört ihr Inhalt zu einer vollständigen Auskunft.

Ehrlich währt am längsten

Was ist, wenn das Unternehmen solche „persönlichen Notizen“ über Kunden ausdrücklich untersagt hat, sie aber trotzdem vorhanden sind? Dann wird die Existenz dieser Notizen gern verschwiegen, wenn das Unternehmen eine Auskunft zusammenstellen lässt. Die Folge: Die Auskunft ist unvollständig! Das kann dem Unternehmen im Ernstfall erheblichen rechtlichen Ärger bescheren.

Die Auskunft ist oft Basis für weitere Ansprüche

Die Datenschutz-Grundverordnung (DSGVO) gewährt den Auskunftsanspruch, damit die betroffene Person weitere Rechte wahrnehmen kann. Stellt die betroffene Person etwa fest, dass Daten in der Auskunft unrichtig sind, wird sie eine Berichtigung dieser Daten verlangen. Auch das dient natürlich dem Datenschutz und ist in Ordnung.

Wo fängt der Missbrauch an?

Manchmal läuft eine Forderung nach Auskunft aber auch ganz anders ab. Ein Beispiel: Ein Kunde verlangt bei einem Unternehmen Auskunft über alle Daten, die ihn betreffen. Dies geschieht, während ein Rechtsstreit – beispielsweise wegen angeblicher Mängel einer Lieferung – schon in der Luft liegt. Dann geht es dem Kunden eher nicht um den Datenschutz. Manchmal sagt ein Kunde in solchen Fällen auch ganz offen, dass er nach zusätzlichem Beweismaterial für einen Rechtsstreit sucht.

Die Gerichte schwanken noch

Ist das Rechtsmissbrauch oder ist das noch o.k.? Darüber sind sich die Gerichte im Augenblick noch nicht einig. Die DSGVO beschränkt den Auskunftsanspruch nicht auf bestimmte Motive. Das spricht gegen einen Missbrauch. Andererseits ist das Ziel der DSGVO der Datenschutz. Sie sollte nie ein Hebel dafür werden, Vertragspartner schikanieren zu können. Auch als Instrument für die Beschaffung von Beweismaterial war sie nie gedacht. Aber wie gesagt: Die Gerichte entscheiden bisher sehr unterschiedlich.

Auskünfte kosten im Normalfall nichts

Besonders heikel ist das vor dem Hintergrund, dass für eine Auskunft normalerweise nichts berechnet werden darf. Eine Ausnahme gilt, wenn ein „exzessiver Antrag“ vorliegt. Das wäre etwa der Fall, wenn jemand in kurzen Abständen mehrfach Auskunft über dieselben Daten verlangt. Das Beispiel zeigt: Solche Ausnahmen sind wirklich selten.

Interne Anweisungen werden strenger

Im Ergebnis müssen sich Unternehmen darauf einstellen, dass sie weitaus häufiger als früher gewohnt umfassend Auskunft erteilen müssen – und das auch noch kostenlos. Der damit verbundene Aufwand ist beträchtlich. Verständlich, dass Unternehmen darauf reagieren. Vielfach legen sie deutlich genauer als bisher durch interne Anweisungen fest, welche Daten die Beschäftigten überhaupt speichern dürfen. Auch die Dauer der Aufbewahrung wird oft strenger geregelt. Alle in einem Unternehmen tun gut daran, solche Vorgaben sorgfältig zu beachten.

4 DRUCKER, DOKUMENTE UND DIGITALE TRANSFORMATION

Auch wenn die Corona-Pandemie die Digitalisierung weiter beschleunigt hat: Papierdokumente spielen weiterhin eine wichtige Rolle und enthalten personenbezogene Daten. Vergessen Sie deshalb bei den Schutzmaßnahmen auch das Papier nicht. Gerade im Homeoffice könnte dies leicht geschehen.

Das digitale Büro bleibt Zukunft

Schon lange wird über das digitale Büro gesprochen: Alles wird digitalisiert, Aktenordner verschwinden. Doch diese Vorstellung ist auch heute noch Zukunftsmusik. Bisher verwenden erst 48 Prozent der Unternehmen Lösungen, um Dokumente zu digitalisieren, wie der Digitalverband Bitkom berichtet hat.

So kommt es auch, dass es weiterhin viele Dokumente in Papierform gibt, die personenbezogene Daten enthalten und die deshalb zu schützen sind. Dabei befinden sich die Papierdokumente nicht nur im verschlossenen Aktenschrank.

Vertrauliche Unterlagen pendeln zwischen Büro und Homeoffice

Viele Papierdokumente werden auch außerhalb des Büros und Firmengebäudes genutzt und aufbewahrt. Die Tätigkeit im Homeoffice und die mobile Arbeit unterwegs haben dies noch verstärkt. Wo in Zukunft die sogenannte Hybride Arbeit als Mischung aus Büro und Homeoffice zum betrieblichen Alltag wird, hat dies auch Folgen für die Papierdokumente.

So transportieren die Beschäftigten dann Akten und andere Dokumente in Papierform zwischen den verschiedenen Arbeitsorten. Es kann etwa sein, dass jemand einen aktuellen Kundenvorgang im Homeoffice ausdruckt und dann später mit ins Büro nimmt, um das Dokument in der entsprechenden Akte abzulegen. Bei diesem Transport jedoch könnte das Dokument verloren gehen oder gar gestohlen werden.

Drucker sind ein mehrfaches Angriffsziel

Aber auch der Ausdruck selbst im Homeoffice birgt Risiken. Viele Drucker werden inzwischen in das WLAN im Homeoffice eingebunden. Manche sind sogar direkt über das Internet zu erreichen, damit man auch unterwegs etwas drucken kann, das dann im Homeoffice wartet.

Cyber-Attacken haben vernetzte Drucker im Visier. Es gibt aktuelle Beispiele, dass Cyberkriminelle Schwachstellen in Verbindung mit Druckern aktiv ausnutzen. Dabei bieten Drucker gleich mehrere Angriffsziele: Angreifer könnten ungeschützte Druckverbindungen abhören, ungeschützte Datenspeicher im Drucker auslesen, dort Malware deponieren und den unzureichend geschützten Drucker als heimli-chen Zugang zum Endgerät und ins Netzwerk nutzen.

Mehr Datenschutz für Dokumente und Drucker

Denken Sie bei der digitalen Transformation deshalb nicht nur an den digitalen Datenschutz, sondern auch an Papierdokumente und an die Drucker, die Dokumente in Papierform ausgeben.

Andernfalls könnten Dokumente und Drucker zum Datenleck werden – sei es bei der unsicheren Lagerung, dem ungeschützten Transport oder der fehlerhaften Entsorgung über den normalen Papiermüll. Auch im Homeoffice und unterwegs müssen angemessene Schutzmaßnahmen verfügbar sein, wie zum Beispiel ein Papierschredder, der dem Schutzbedarf der Dokumente, die entsorgt werden sollen, entspricht.

Denken Sie nicht zuletzt daran, dass der Schreibtisch im Homeoffice kein sicherer Ort ist,

um Akten aufzubewahren. Ein Homeoffice-Arbeitsplatz kann viel mehr „Publikumsverkehr“ haben als so manches Büro.

Haben Sie Ihre Papierdokumente im Griff? Machen Sie den Test!

Der Datenschutz betrifft nur Dateien, nicht aber Papierdokumente. Stimmt das?

1. Nein, auch Papierdokumente können zu schützende personenbezogene Daten enthalten.
2. Ja, denn der Datenschutz gilt nur für die automatisierte Verarbeitung personenbezogener Daten.

Lösung:

Die Antwort 1. ist richtig. Die Datenschutz-Grundverordnung (DSGVO) gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten, aber auch für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Unter Dateisystem versteht die DSGVO jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, also zum Beispiel auch gedruckte Kundenlisten in einem Aktenordner.

Drucker im Homeoffice sind über das Internet nicht zu erreichen. Stimmt das?

1. Ja, ist die Tür zum Homeoffice abgeschlossen, kann niemand an den Drucker.
2. Nein, über WLAN und teils über das offene Internet könnten Drucker für Angreifer erreichbar sein.

Lösung:

Die Antwort 2. ist richtig. Inzwischen werden gerade im Homeoffice die meisten Drucker über WLAN angebunden. Schwachstellen im WLAN könnten damit Dritten Zugang zum Drucker und den darauf gespeicherten Druckdaten geben. Zudem bieten viele Druckermodelle eine direkte Verbindung ins Internet und haben eine eigene E-Mail-Adresse. Das macht es möglich, von unterwegs über das Internet darauf zu drucken. Damit sind aber auch Cyberattacken auf diese Drucker möglich. Die Daten, die auf der Festplatte des Druckers liegen, könnten auf diesem Weg ebenso in Gefahr geraten wie die Daten, die für einen Ausdruck auf den Drucker temporär übermittelt werden.

IMPRESSUM

Redaktion

Dr. Uwe Günther
Sanovis GmbH
Riedenburger Straße 7
81677 München
089 9927579-22
Uwe.Guenther@Sanovis.com

Stefan Strüwe, RA
CURACON GmbH Wirtschaftsprüfungsgesellschaft
Am Mittelhafen 14
48155 Münster
0251 92208-209
Stefan.Struewe@Curacon.de